IN THE CLAIMS:

Please amend claims 1, 2, 4-15 and 18-22 as follows:

1. (Currently Amended) Authentication method for telecommunication networks, especially for IP networks, in accordance with which method the identity of a subscriber attached to the network is authenticated,

characterized by:

in a network terminal ~~(TEI)~~, using a subscriber identity module ~~(SIM)~~ essentially of the same kind as in a known mobile communications system ~~(MN)~~, which identity module is such that a response is obtained as a result of a challenge given to it as input,

using a special security server ~~(SS)~~ in the network so that when a terminal attaches to the network, a message of a new user is transmitted to the security server,

fetching subscriber authentication information corresponding to the ~~said~~ new user from the ~~said~~ mobile communications system to the ~~said~~ network, which authentication information contains at least a challenge and a response, and

performing ~~the~~ authentication based on the authentication information obtained from the mobile communications system by transmitting the ~~said~~ challenge to the terminal through the network, by checking that the challenge is unique from challenges used in previous authentication exchanges, by generating, if the challenge is unique, the ~~a~~ response from the challenge in the identity module of the terminal and by comparing the response with the response received from the mobile communications system.

2. (Currently Amended) Method as defined in claim 1, characterized in that fetching of the subscribers authentication information from the mobile communications system is started from the security server ~~(SS)~~ in response to the ~~said~~ message.

3. (Original) Method as defined in claim 1, characterized in that in response to a successful authentication, registration of the subscriber is performed as a client of a separate key management system.

4. (Currently Amended) Method as defined in claim 3 ~~for IP networks~~, characterized in that ~~the~~ a known Kerberos system is used as the key management system.

5. (Currently Amended) Method as defined in claim 4, characterized in that the subscriber-specific authentication information obtained from the mobile communications system also includes a key ~~(Kc)~~, whereby the subscriber is registered as a client of the Kerberos system so that the key is registered (a) as the clients password and (b) as a password for a service formed for the clients IP address or for a subscriber identity ~~(IMSI)~~ used in the mobile communications system.

6. (Currently Amended) Method as defined in claim 1, characterized in that the subscribers authentication information is fetched with the aid of a separate proxy server ~~(HP)~~, which functions as a network element emulating ~~the~~ a visitor location register ~~VLR~~

of the mobile communications system and which requests the authentication information from an authentication ~~centre~~ center ~~AuC~~ located in connection with ~~the~~ a subscribers home location register ~~HLR~~ in the same way as the mobile communications system's own visitor location register.

7. (Currently Amended) Method as defined in claim 1, characterized in that the subscribers authentication information is fetched with the aid of a separate proxy server ~~(BP)~~, which functions as a network element emulating the mobile communications system's base station controller and which is in connection with the mobile communications system's mobile switching centre ~~(MSC)~~ for fetching the authentication information from an authentication ~~centre~~ center ~~AuC~~ located in connection with ~~the~~ a subscribers home location register ~~HLR~~ in the same way as the authentication information is fetched to the mobile communications system's own base station controller.

8. (Currently Amended) Authentication system for telecommunications networks, especially for IP networks, which system includes authentication means for authenticating the identity of a subscriber who has attached to the network,

characterized in that the authentication means include

a subscriber identity module ~~(SIM)~~ connected to the network's terminal ~~(TEI)~~, the module being essentially similar to the subscriber identity module used in a

separate mobile communications system ~~(MN)~~, whereby a response can be determined from a challenge given to the identity module as input,

messaging means ~~(HA)~~ for sending a message when a terminal attaches to the network,

a special security server (SS) for receiving the ~~said~~ message,

means for requesting authentication information corresponding to a subscriber from the ~~said~~ mobile communications system ~~(MN)~~, which information contains at least a challenge and a response, and

on the side of the ~~said~~ network, data transmission and checking means for transmitting the challenge through the network to the identity module and for checking that the challenge is unique from challenges used in previous authentication exchanges, for returning the response from the terminal to the network, if the challenge is unique, and for comparing the received response with the response received from the mobile communications system.

9. (Currently Amended) System as defined in claim 8,characterized in that the ~~said~~ identity module is the subscriber identity module ~~(SIM)~~ used in the GSM network.

10. (Currently Amended) System as defined in claim 8, characterized in that the messaging means are adapted into a home agent ~~(HA)~~ in accordance with the mobile IP network.

11. (Currently Amended) System as defined in claim 8,characterized in that the means for requesting authentication information include the ~~said~~ security server and a proxy server ~~(HP, BP)~~, which is connected to the GSM network.

12. (Currently Amended) System as defined in claim 11, characterized in that the proxy server functions as a network element emulating the visitor location register ~~VLR~~ of the GSM network.

13. (Currently Amended) System as defined in claim 11, characterized in that the proxy server functions as a network element emulating the base station controller ~~BSC~~ of the GSM network.

14. (Currently Amended) System as defined in claim 11, characterized in that the system further includes a Kerberos server ~~(KS)~~ which is known as such and as the user of which the subscriber will be registered as a result of a successful authentication.

15. (Currently Amended) Authentication method for telecommunications networks, especially for IP networks, in accordance with which method the identity of a subscriber attached to the network is authenticated,

characterized by

in a network terminal ~~(TEl)~~, using a subscriber identity module ~~(SIM) 25~~ essentially similar to the one used in a known mobile communications system ~~(MN)~~, which identity module is such that a response is obtained as a result of a challenge given to it as input,

storing subscriber-specific authentication information in a database ~~(DB)~~, the information being in that way essentially similar to the information used for authentication in the ~~said~~ mobile communications system that it contains at least a challenge and a response,

using a special security server ~~(SS)~~ in the network so that when a terminal attaches to the network, a message about the new user is transmitted to the security server,

in response to the message, retrieving authentication information of the subscriber corresponding to the new user from the ~~said~~ database ~~(DB)~~, and

performing authentication based on the authentication information obtained from the database by transmitting the ~~said~~ challenge through the network to the terminal, by checking that the challenge is unique from challenges used in previous authentication exchanges, by generating, if the challenge is unique, a response from the challenge in the identity module of the terminal, and by comparing the response with the response obtained from the database.

16. (Original) Method as defined in claim 15, characterized in that the database is stored

in connection with the security server.

17. (Original) Method as defined in claim 15, characterized in that in response to a successful authentication, registration of the subscriber is performed as the user of a separate key management system.

18. (Currently Amended) Method as defined in claim 17, characterized in that ~~the~~ a known Kerberos system is used as the key management system.

19. (Currently Amended) Authentication system for telecommunications networks, especially for IP networks, which system includes authentication means for authentication of the identity of a subscriber attached to the network,

characterized in that the authentication means include

a subscriber identity module ~~(SIM)~~, which is connected to a network terminal ~~(TEI)~~ and which is essentially similar to the subscriber identity module used in a separate mobile communications system ~~(MN)~~, whereby a response can be determined from the challenge given as input to the identity module,

messaging means ~~(HA)~~ for sending a message when a terminal attaches to the network,

a special security server ~~(SS)~~ for receiving the ~~said~~ message,

database means ~~(SS, DB)~~, which include a database ~~(DB)~~, wherein

subscriber-specific authentication information is stored, which is in such a way essentially similar to the information used for authentication in the ~~said~~ mobile communications system that it includes at least a challenge and a response, and retrieval means ~~(SS)~~ for retrieving subscriber-specific authentication information from the ~~said~~ database in response to the message, and

on the side of the ~~said~~ network, data transmission and checking means for transmitting the ~~said~~ challenge through the network to the identity module and for checking that the challenge is unique from challenges used in previous authentication exchanges, if the challenge is unique, for returning the response from the terminal to the network, and for comparing the received response with the response received from the database.

20. (Currently Amended) System as defined in claim 19, characterized in that the ~~said~~ identity module is a subscriber identity module ~~(SIM)~~ used in the GSM network.

21. (Currently Amended) System as defined in claim 19, characterized in that the messaging means are adapted into a home agent ~~(HA)~~ in accordance with the mobile IP network.

22. (Currently Amended) System as defined in claim 19, characterized in that the system further includes a Kerberos server ~~(KS),~~ which is known as such and as the client of

which the subscriber is registered as the result of a successful authentication.